

КРИМИНАЛИСТИКА И КРИМИНОЛОГИЯ. СУДЕБНАЯ ЭКСПЕРТИЗА

DOI: 10.17803/1994-1471.2022.136.3.102-111

А. Б. Смушкин*

Криминалистические аспекты исследования даркнета в целях расследования преступлений

Аннотация. Объектом исследования является специфическая информационная структура — даркнет, а также криминалистические аспекты его изучения в ходе расследования. В статье дается краткий обзор особенностей уровней интернета: Clearnet, Deepnet и Darknet. С учетом специфики даркнета констатируется сложность расследования преступлений, совершенных с его использованием. Определяется примерный список совершаемых через даркнет преступлений. Указывается на существование двух основных программных комплексов для работы в даркнете: 2IP и TOR. Автор при рассмотрении специфики работы 2IP как одно-ранговой пиринговой сети констатирует, что без агентурной работы вхождение в число пользователей сети или внешний взлом практически невозможны. В статье кратко излагаются принцип работы TOR (The Onion Router), особенности многоуровневого шифрования и опасность возложения ответственности на владельца выходного узла маршрута. Предлагаются оперативно-розыскные, криминалистические и программные меры деанонимизации пользователей в целях расследования.

Ключевые слова: интернет; даркнет; TOR; луковичная маршрутизация; расследование; деанонимизация пользователей даркнета; исследование незаконных действий в даркнете; оперативно-розыскные мероприятия в даркнете; пиринговые сети; криминалистика; электронная цифровая криминалистика; сетевая криминалистика.

Для цитирования: Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. — 2022. — Т. 17. — № 3. — С. 102–111. — DOI: 10.17803/1994-1471.2022.136.3.102-111.

© Смушкин А. Б., 2022

* Смушкин Александр Борисович, кандидат юридических наук, доцент, доцент кафедры криминалистики Саратовской государственной юридической академии, доцент кафедры уголовного права и процесса Поволжского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России) в г. Саратове
ул. Вольская, д. 1, г. Саратов, Россия, 410056
skif32@yandex.ru

Forensic Aspects of the Dark Net Study for Crimes Investigation Purposes

Aleksandr B. Smushkin, Cand. Sci. (Law), Associate Professor, Associate Professor, Department of Criminalistics, Saratov State Law Academy; Associate Professor, Department of Criminal Law and Procedure, the Volga Region Institute (Branch) of the All-Russian State University of Justice (RLA of the Ministry of Justice of Russia), Saratov
ul. Volskaya, d. 1, Saratov, Russia, 410056
skif32@yandex.ru

Abstract. The object of the study is a specific information structure — the dark net — and forensic aspects of its study during the investigation. The paper gives a brief overview of the features of the Internet layers: Cleernet, Deepnet and Darknet. Taking into account the specifics of the dark net, the complexity of investigating crimes committed with its use is stated. An approximate list of crimes committed through the dark net is determined. The existence of two main software systems for working in the dark net is indicated: 2IP and TOR. The author, when considering the specifics of the work of 2IP as a peer-to-peer network, states that without undercover work, becoming a network users or external hacking are practically impossible. The paper briefly outlines the principle of TOR (The Onion Router) operation, the features of multi-level encryption and the danger of imposing responsibility on the owner of the route exit node. The author suggests implementing operation and search, forensic and software measures to deanonymize users for the investigation purpose.

Keywords: Internet; dark net; TOR; onion routing; investigation; deanonymization of dark net users; investigation of illegal activities on dark web; operation and search activities in the dark net; peer networks; criminalistics; electronic digital forensics; network forensics.

Cite as: Smushkin AB. Kriminalisticheskie aspekty issledovaniya darkneta v tselyakh rassledovaniya prestupleniy [Forensic Aspects of the Dark Net Study for Crimes Investigation Purposes]. *Aktual'nye problemy rossijskogo prava*. 2022;17(3):102-111. DOI: 10.17803/1994-1471.2022.136.3.102-111. (In Russ., abstract in Eng.).

Современный период развития общественных, в том числе общественно-политических отношений, характеризуется особым вниманием всех участников к информации, коммуникации и защите конфиденциальности данных (объектов и процессов). Активно используются при этом как региональные сети, так и международная сеть Интернет.

Существенный объем научной, политической, деловой, а также криминальной коммуникации переместился сейчас в телекоммуникационные сети. При этом в настоящий момент основное внимание в научных исследованиях и практике правоохранительной деятельности уделяется мониторингу, контролю и противодействию преступным проявлениям в открытых источниках. Между тем открытые источники интернета представляют собой лишь поверхностный слой, пусть и глобальный, всей телекоммуникационной сферы.

Современный интернет представляет собой неоднородную систему. Большинство авторов сходятся в выделении трех основных уровней/слоев/видов интернета:

- 1) открытый интернет — Cleernet, Surfacenet, Clearweb;
- 2) глубокий интернет — Deepnet, Deepweb;
- 3) темный, теневой интернет — Darknet, Darkweb.

Cleernet представляет собой самый распространенный уровень интернета. Все источники в нем индексируются. Практически все являются неанонимными, требующими авторизации. Не требуется специальное программное обеспечение. Используется широкий спектр браузеров и не предпринимаются меры по анонимизации интернет-серфинга. Однако, по статистике, открытый интернет содержит всего около 5 % информации и интернет-ресурсов всей Сети¹.

¹ Что такое глубокий и теневой интернет? // URL: <https://kaspersky-ru.turbopages.org/kaspersky.ru/s/resource-center/threats/deep-web> (дата обращения: 22.04.2021).

Deepnet и Darknet некоторые авторы объединяют в одну категорию «глубокий интернет» или указывают на то, что понятие «глубокий интернет» является широким, включающим в себя и теневой². В частности, такой позиции придерживаются специалисты лаборатории Касперского³.

Однако такое слияние в одну категорию нам представляется технически и методически ошибочным. Каждый из этих видов обладает достаточным объемом эмерджентных свойств для их дифференциации. Так, Deepnet представляет собой совокупность корпоративных и иных сетей, баз данных, не индексируемых в открытом интернете, однако и не анонимизирующих пользователей. Для их использования применяется обычное программное обеспечение. По некоторым данным, такие сети занимают около 70 % всего интернета.

Darknet, Darkweb (темный интернет) — это ряд сетей, акцентирующих анонимизацию пользователей. Данные сети не индексируются в открытом интернете. Для их использования необходимо специальное программное обеспечение. Еще одной специфической чертой даркнета является туннелирование трафика. Именно Darknet является основным объектом нашего исследования.

Анонимизация пользователей может использоваться как для вполне законных целей (защиты тайны личной жизни, тайны переписки и так далее), так и для нелегальной и даже противозаконной деятельности. Даркнет по разным оценкам ученых занимает от 0,1 до 1 % всего интернета⁴. Однако объем его криминального использования очень велик. По оценке исследо-

вателей, к основным противозаконным направлениям использования даркнета относятся:

- 1) преступная деятельность, связанная с незаконным контентом сексуального характера;
- 2) преступная деятельность, связанная с оборотом наркотиков;
- 3) преступная деятельность, связанная с оборотом компьютерной информации (включает в себя многочисленные действия, касающиеся неправомерного доступа к информации);
- 4) преступная деятельность в сфере экономики (этот вид преступности включает в основном действия, связанные с оборотом поддельных банковских карт и их данных);
- 5) преступная деятельность экстремистской направленности;
- 6) преступная деятельность, связанная с оборотом поддельных документов;
- 7) преступная деятельность, связанная с оборотом оружия;
- 8) преступная деятельность, связанная с насилием;
- 9) преступная деятельность, связанная с нарушением прав интеллектуальной собственности⁵.

Следует также упомянуть про так называемые красные комнаты (Red Room) — скрытые видеоканалы сети Darknet, где в прямом эфире показываются реальные пытки и насилие⁶.

Выход в даркнет осуществляется с помощью специального программного обеспечения TOR (The Onion Router), 2IP (Invisible Internet Project — невидимый интернет) и др.

Сети, основанные на технологии 2IP, функционируют посредством полной децентрализации пиринговых сетей. Каждый из пользова-

² Сетько А. А., Швец Ю. Н. Darknet — одна из сторон интернета // Наука — образованию, производству, экономике : материалы XXII (69) Региональной научно-практической конференции преподавателей, научных сотрудников и аспирантов : в 2 т. Витебск : Изд-во Витебского государственного университета имени П. М. Машерова, 2017. С. 79.

³ Что такое глубокий и теневой интернет?

⁴ Васильев А., Ибрагимов Ж., Васильева О. Даркнет как ускользящая сфера правового регулирования // Юрислингвистика. 2019. № 12. С. 11.

⁵ Узденов Р. М. Новые границы киберпреступности // Всероссийский криминологический журнал. 2016. Т. 10. № 4. С. 651.

⁶ Красные комнаты Даркнета — что это и как туда попасть? // URL: <https://darkstack.pro/dark-web/red-room-darknet/> (дата обращения: 01.05.2021).

телей является и сервером, и клиентом. Такая система крайне устойчива к внешнему влиянию со стороны тех же правоохранительных органов, поскольку вмешаться извне в одноранговую сеть с ограниченным доступом практически невозможно. Для проникновения в сеть, изучения и изъятия информации в целях доказывания сотрудники правоохранительных органов должны максимально использовать агентурные сети и легендированный ввод, внедрение сотрудника в число пользователей или получение доступа к учетной записи (логину и паролю) действующих пользователей.

Наиболее распространенными являются сети, основанные на применении специализированного программного обеспечения TOR, поэтому в исследовании мы уделяем особое внимание именно ему. TOR представляет собой гибридную сеть, имеющую элементы и централизованной, и одноранговой. Высказываются различные мнения относительно возможности деанонимизации в целях расследования пользователей TOR, от «практически нереально», до «сложно, но можно». Представляется, что истина находится где-то посередине. В августе 2015 г. МВД РФ подписывало контракт с отечественной фирмой на разработку возможностей взлома сети TOR⁷. Однако исполнитель не сумел выполнить контракт в срок⁸.

Для рассмотрения криминалистических аспектов исследования даркнета необходимо изложить общие принципы работы TOR. Он работает с конкретной группой сайтов с расширением .onion. Функционирование TOR основано на многослойном шифровании и многоступенчатой передаче данных. Специфика данного программного комплекса состоит в повышенной анонимизации участников. При его использовании информация упаковывается в несколько

слоев шифра, применяются несколько групп компьютеров-ретрансляторов. Как указывают Ю. А. Бондаренко и Г. М. Кизилов, «маршрутизатор вначале передачи информации выбирает случайное число промежуточных маршрутизаторов и генерирует CREATE-сообщения, шифруя их симметричным ключом и указывая для каждого маршрутизатора, какой маршрутизатор будет следующим на пути»⁹. Таким образом, между компьютерами пользователей и компьютерами получателей информации имеется как минимум три промежуточных пункта (так называемые ноды). Первый пункт, входной узел (entry), — это компьютер, данные которого присланы при подключении TOR. Как отмечает А. В. Лазаренко, «к узлам, выбираемым системой в качестве входных, предъявляются особые требования: они должны быть в сети достаточно давно (восемь дней), обладать высокой пропускной способностью, хорошей производительностью»¹⁰. На этом компьютере распаковывается первый слой шифра, раскрывается информация, касающаяся следующего звена, однако при этом источник информации еще открыт, но получатель анонимен.

Центральное звено (мидл) IP-адреса отправителя уже не видит, адрес получателя также находится в другом слое. Для подобной переделки используются добровольно предоставляемые любыми пользователями IP-адреса и мощности их компьютеров.

Третья же нода — выходной узел (exit) — распаковывает информацию о получателе, не видя источника. Таким образом, источник трафика не выявляется на стороне получателя, а адресат не виден на стороне источника.

Практика отечественной правоохранительной деятельности показывает слабую техническую подготовленность к работе в подобной

⁷ МВД подписало контракт на проведение исследований возможности взлома анонимной сети Tor // URL: <http://www.securitylab.ru/news/456957.php> (дата обращения: 25.04.2021).

⁸ Коломыченко М. TOR хозяйствующих субъектов // Коммерсантъ. 2015. URL: <https://www.kommersant.ru/doc/2861002> (дата обращения: 25.04.2021).

⁹ Бондаренко Ю. А., Кизилев Г. М. Проблемы выявления и использования следов преступлений, оставляемых в сети Darknet // Гуманитарные, социально-экономические и общественные науки. 2019. № 5. С. 99.

¹⁰ Лазаренко А. В. Технологии деанонимизации пользователей TOR // Новые информационные технологии в автоматизированных системах. 2016. № 19. С. 257.

среде. Подмена источника информации промежуточной нодой приводит зачастую к ошибочному вовлечению в сферу уголовного судопроизводства владельцев промежуточных терминалов. Например, математика Дмитрия Богатова едва не привлекли к уголовной ответственности за экстремистские публикации в сети Интернет, притом что он был не непосредственным автором публикации, а владельцем выходного узла¹¹. Однако при этом некоторые авторы продолжают рекомендовать борьбу с незаконным контентом в Darknet с помощью поиска администратора выходного узла¹². Представляется необходимым не просто участие в раскрытии и расследовании специалистами отделов по борьбе с высокотехнологическими преступлениями (отделов «К»), но также привлечение сотрудников специализированных компаний в сфере информационно-коммуникационных технологий: Group-IB, «Лаборатория Касперского» и т.д.

Нам представляется, что борьба с даркнетом может быть кардинальной, с помощью блокирования выхода на уровне страны индивидуальных пользователей, поскольку список нод известен, либо с полной блокировкой по типу «Великого китайского файрвола»¹³, а также адресной. По смыслу изменений, внесенных в законодательство Федеральным законом от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”»¹⁴, доступ к TOR на территории Российской Федерации должен быть ограничен. С помощью этого закона предполагалось установить запрет обхода блокировок с помощью различных ано-

нимайзеров. Однако подобные ресурсы, расположенные за пределами РФ, едва ли будут следовать данной норме и сотрудничать с российскими правоохранительными органами.

Универсальная блокировка не является панацеей и обходится с помощью «мостов», «зеркал», VPN-серверов.

К таким же малореальным методам, на наш взгляд, относится и модификация программного обеспечения, идея которого заключается в преобразовании изначального программного кода TOR, с тем чтобы браузер сам присылал информацию о путях передачи информации или облегчал взлом. Подобный коррумпированный дистрибутив TOR должен быть размещен на подавляющем большинстве источников, откуда скачиваются дистрибутивы.

Попытки определения методик борьбы с даркнет-преступностью в TOR были предприняты исследовательским институтом RAND Europe. Специалисты данного института выделили следующие методы:

- 1) традиционные методы расследования, применяемые в наркотической цепочке (например, наблюдение, тайные операции);
- 2) обнаружение и перехват почты (например, сотрудничество между правоохранительными органами и почтовыми службами);
- 3) онлайн-обнаружение (например, методы больших данных, мониторинг онлайн-рынков, отслеживание денежных потоков);
- 4) онлайн-дезорганизация (например, закрытие онлайн-рынков)¹⁵.

Однако данные методы лишь указывают направления деятельности, а не предлагают

¹¹ Тадтаев Г., Костина Е. В деле математика Богатова сменился обвиняемый // Сайт RBC. URL: https://rbc.ru/turbopages.org/turbo/rbc.ru/s/society/21/05/2018/5b029a299a79470316d5afba?utm_source=turbo_turbo (дата обращения: 25.04.2021).

¹² Каримов В. Х. Актуальные вопросы выявления и расследования преступлений, совершаемых с использованием средств шифрования данных в сети Интернет // Уголовно-процессуальные и криминалистические чтения на Алтае : сборник науч. статей. Вып. 14 «Проблемы противодействия киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами». Барнаул : Изд-во АлтГУ. 2017. С. 40–48.

¹³ Что такое глубокий и теневой интернет?

¹⁴ СЗ РФ. 2017. № 31. Ст. 4825.

¹⁵ Taking Stock of the Online Drugs Trade / S. Hoorens, K. Kruithof [et al.] // URL: <https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html> (дата обращения: 23.04.2021).

конкретные шаги. Нам представляется, что некоторые идеи являются преимущественно декларативными, а не реальными.

Большинство сайтов Darknet, связанных с криминальными товарами или услугами, представляет собой торговые площадки, предоставляющие возможность продавцам выставить свой товар. Следовательно, интересующими правоохранительные органы фигурантами могут стать: администратор (или собственник) торговой площадки, продающей нелегальный товар, продавец товара и покупатель товара.

Основную роль в исследовании незаконных действий в Darknet должны играть оперативно-розыскные методы и средства. Мы полагаем, что для получения криминалистически значимой информации, расследования и пресечения противозаконной деятельности возможно использование направлений исследования, условно называемых нами «от сайта» или «от пользователя».

Содержимое «торговых площадок» может быть зафиксировано с помощью осмотра сайта. Добровольность выставления и осведомленность о незаконном содержимом конкретных предлагаемых объектов может подтверждаться изучением правил пользования сайтом, а также проведением оперативно-розыскного мероприятия «Проверочная закупка». Однако на первый план в любом случае выдвигается вопрос по деанонимизации администраторов торговой площадки и продавцов.

В первую очередь необходимо отслеживать активность модераторов (владельцев)

криминальных ресурсов даркнета в обычном интернете (Clearnet). Зачастую первичный поиск клиентов для криминального бизнеса ведется в открытой сети или в «Телеграм». Представляется возможным в подобной ситуации рекомендовать применение методов OSInt (Open Source Intelligence — разведка на основе открытых источников)¹⁶.

Известен факт, что администратор одной из самых распространенных сетей торговли криминальным товаром Silk Road Рос Ульбрихт, не скрывая своих данных, пользовался для рекламы мессенджерами и социальными сетями открытого интернета, выходил в Сеть из ближайшего к дому интернет-кафе, для связи оставлял адрес электронной почты rossulbricht@gmail.com¹⁷. Подобная беспечность в области сетевой гигиены позволила принять меры по его выявлению и задержанию. В США действуют специализированные мониторинговые центры, отслеживающие информацию об анонимных веб-ресурсах и даркнет-сервисах (например, DeepDotWeb, All Things Vice)¹⁸.

Определенную роль может играть отслеживание денежных потоков и контроль подозрительных сделок, однако преступники, работающие в Darknet, чаще используют не реальные денежные средства, пусть и с помощью онлайн-сервисов, а их электронные анонимные суррогаты или вообще финансовые активы, созданные с применением блокчейн-технологий: токены¹⁹ и кибервалюты²⁰. Применение блокчейн-технологий делает практически недо-

¹⁶ Подробнее см., например: Конкурентная разведка в компьютерных сетях / А. Г. Додонов, Д. В. Ландэ [и др.]. Киев : ИПРИ НАН Украины, 2013 ; Воксанаев В. П. Разведка по открытым источникам: уроки прошлого. Рязань : Поверенный, 2007.

¹⁷ Каримов В. Х. Указ. соч. С. 43.

¹⁸ См.: Жмуров Д. В. Даркнет как ускользающая сфера правового регулирования // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 1 (27). С. 96.

¹⁹ Цифровая виртуальная финансовая единица с преимущественно централизованной эмиссией конкретным физическим или юридическим лицом или группой лиц, в которую вложен определенный материальный актив из реального мира, действующая на блокчейн-платформе какой-либо кибервалюты. Выделяют следующие виды: токены приложений (для оплаты внутренних сервисов приложений), кредитные токены (предназначены для инвестиций и получения пассивного дохода), asset-backed tokens (токены, подтвержденные реальными физическими активами).

²⁰ Полностью виртуальные платежные средства с децентрализованной эмиссией, функционирующие на основе собственной блокчейн-платформы.

ступным отслеживанием движения финансовых средств.

При движении «от сайта» возможна организация копии известного сайта, например «Шелковый путь», или «Гидра», или создание самостоятельных, не раскрученных onion-сайтов с целью обеспечения оперативного эксперимента. В дальнейшем возможно отслеживание почтового заказа или доставки путем контролируемой поставки. Кроме того, при надлежащем налаженном взаимодействии с почтовыми и курьерскими службами возможно своевременное выявление заказанного подозрительного отправления.

При нематериальном заказе или получении с сайта определенной информации, налаживании коммуникаций возможно использование стеганографической закладки или компьютерного червя с целью отслеживания пути движения информации и адресата.

В случае использования некоторых поисковиков и почтовых систем возможен взлом сайта или почтовых программ. Так, с помощью программного комплекса «Мобильный криминалист» возможно изъять и исследовать информацию поисковика DDG (DuckDuckGo), если он применяется для поиска в Darknet. Этот же аппаратно-программный комплекс позволяет анализировать информацию широко распространенного в Darknet почтового клиента Secmail²¹.

Необходимо подчеркнуть и важность оптимальной организации агентурной работы. Многие сайты даркнета требуют так называемых приглашений (инвайтов) от доверенных пользователей для доступа к сайту. Для получения инвайта необходимо использовать активную агентуру. Кроме того, возможен вход под учетной записью агента-осведомителя.

Возможно также внедрение сотрудника в группу пользователей сайта и таким образом

получение доступа к сайту. После получения доступа к сайту может быть организована проверочная закупка.

При поиске «от заказчика», «от клиента» используется информация провайдера о подключении к входной ноде. Может быть сопоставлено время выхода в Darknet, подключения к входной ноде и появления определенного преступного результата, преступного события. В большинстве случаев будут получены косвенные доказательства, которые должны оцениваться в совокупности. Кроме того, эффективность данного метода повышается только в случае, если уже имеется подозреваемый, действия которого в киберпространстве отслеживают правоохранительные органы. В отношении заподозренного лица устанавливается наблюдение. С помощью контроля почтовых отправлений, телеграфных и иных сообщений проверяются заказанные заподозренным объекты.

Представляется мало реальной отработка всего массива лиц, входящих в Darknet, даже в городах среднего размера, не говоря уже о миллионниках или городах федерального значения.

Для взлома трафика в TOR нам представляется необходимым прибегать к использованию нейросетей, обрабатывающих информацию по технологии больших данных (Big Data). Под большими данными понимается «обозначение структурированных и неструктурированных данных огромных объемов и значительного многообразия, эффективно обрабатываемых горизонтально масштабируемыми программными инструментами»²². В другом нормативном акте большие данные определяются как совокупность технологий обработки информации для получения информации, характеристик или вызовов, которые отличают большие данные от простых данных, по общему соглашению три:

²¹ Бой с тенью // Сайт компании «Оксиджен Софтвар». URL: <https://www.oxygensoftware.ru/ru/news/articles/341-darknet> (дата обращения: 24.04.2021).

²² Распоряжение Правительства РФ от 17.12.2019 № 3074-р «Концепция создания цифровой аналитической платформы» (вместе с «Концепцией создания цифровой аналитической платформы предоставления статистических данных») // Сайт Правительства РФ. URL: <http://static.government.ru/media/files/4YejV8mvcCSeGWTg2kXprmthtNbWyfrU.pdf> (дата обращения: 21.04.2021).

volume — объем, velocity — скорость сбора, variety — разнообразие данных»²³.

Большие данные могут быть упорядоченными и неупорядоченными. В рассматриваемом случае особое значение приобретает анализ неупорядоченных больших данных. Естественно, необходим определенный объем накопленных данных, на базе которых активно используется технология машинного обучения Machine Learning. Достаточно крупный объем больших данных постепенно повышает результативность отслеживания и расшифровки трафика. Необходимо развивать и технологии DPI — глубокого анализа пакетов трафика.

Следует также отметить необходимость обязательного исследования постоянной памяти и снятия дампа оперативной памяти у компьютеров обыскиваемых подозреваемых лиц, которые, по имеющейся информации, активно использовали даркнет для совершения преступлений. Для снятия дампа оперативной памяти при этом возможно не только исследование на самом компьютере подозреваемого до снятия планки памяти, но и применение метода «Атака холодом» (Frost Attack) для перестановки планки памяти на другое устройство и исследования на устройстве специалиста. В ходе обыска могут быть обнаружены и электронные следы в виде файла с записями паролей и сайтов или аналогичные бумажные записи, сохраненные в браузере пароли и т.д.

В ходе допроса задержанных пользователей может быть получена информация об источниках незаконных товаров, способах связи, адресах в открытом интернете и даркнете, учетных данных записи пользователя, воспользовавшись которыми, а также внезапностью и сокрытием

задержания подозреваемого, можно проникнуть в интересующие следствие сети.

Зарубежные авторы упоминают также о возможностях специальной программы поискового робота (WebCrawler), который исследует как открытый интернет, так и скрытую сеть интернет-соединений Darknet на предмет совпадений и следов с целью определения возможного участия в незаконной деятельности²⁴.

Кроме того, возможно применение ряда методов, рекомендуемых специалистами. Ю. А. Бондаренко и Г. М. Кизилов, проанализировав работы западных ученых, методы взлома и деанонимизации пользователей TOR, разделили действия на пассивные и активные.

«Пассивные:

- анализ трафика пользователя, основанный на установлении временной взаимосвязи между запросом на создание соединения и установкой выходного соединения;
- другие, основанные на анализе трафика и нагрузки узла внутри сети.

Активные действия:

- комбинированные действия Timing;
- действия Tagging — дублирование случайного сообщения на входном узле, его поиск в поступивших на выходной узел данных;
- Raptor — серия действий по асимметричному анализу трафика, сбору и обработке информации о перебоях, которые приводят в силу специфики топологии и протоколов работы анонимной сети данные на нужный узел, с последующим собиранием проходящего трафика»²⁵.

Расширенный объем программных методов деанонимизации пользователей TOR предлагает и А. В. Лазаренко²⁶.

²³ Распоряжение Минпросвещения России от 18.05.2020 № Р-44 «Об утверждении методических рекомендаций для внедрения в основные общеобразовательные программы современных цифровых технологий» // Законы, кодексы и нормативные правовые акты Российской Федерации. URL: <https://legalacts.ru/doc/rasporjazhenie-minprosveshchenija-Rossii-ot-18052020-n-r-44-ob-utverzhenii/> (дата обращения: 22.04.2021).

²⁴ Techniques and Applications for Crawling, Ingesting and Analyzing Blockchain Data / E. Brinckman, A. Kuehlkamp [et al.] // URL: https://www.researchgate.net/publication/335989766_Techniques_and_Applications_for_Crawling_Ingesting_and_Analyzing_Blockchain_Data (дата обращения: 03.05.2021).

²⁵ Бондаренко Ю. А., Кизилов Г. М. Указ. соч. С. 99.

²⁶ Лазаренко А. В. Указ. соч. С. 262.

В ходе решения основной задачи расследования должны быть выявлены сайты с противозаконным контентом и их владельцы. Должна быть обнаружена и конфискована вся инфраструктура противозаконного сайта, все его серверы. Так, немецкая полиция в ходе закрытия криминального рынка DarkMarket обнаружила и изъяла свыше 20 серверов²⁷.

Таким образом, следует подчеркнуть важность дальнейшего всестороннего изучения такого сетевого феномена, как Darknet, мето-

дов деанонимизации пользователей данной сети, оперативно-розыскного сопровождения и расследования преступлений, совершаемых на просторах Darknet или с его помощью. Важно подчеркнуть необходимость привлечения к расследованию представителей специализированных компаний по расследованию компьютерных инцидентов (Group IB, «Лаборатория Касперского» и т.д.), а также иных признанных специалистов в рассматриваемой сфере.

БИБЛИОГРАФИЯ

1. Бой с тенью // Сайт компании «Оксиджен Софтвр». — URL: <https://www.oxygensoftware.ru/ru/news/articles/341-darknet> (дата обращения: 24.04.2021).
2. Бондаренко Ю. А., Кизилов Г. М. Проблемы выявления и использования следов преступлений, оставляемых в сети Darknet // Гуманитарные, социально-экономические и общественные науки. — 2019. — № 5. — С. 97–101.
3. Васильев А., Ибрагимов Ж., Васильева О. Даркнет как ускользающая сфера правового регулирования // Юрислингвистика. — 2019. — № 12. — С. 11–13.
4. Воксанаев В. П. Разведка по открытым источникам: уроки прошлого. — Рязань : Поверенный, 2007. — 174 с.
5. Конкурентная разведка в компьютерных сетях / А. Г. Додонов, Д. В. Ландэ [и др.]. — Киев : ИПРИ НАН Украины, 2013. — 250 с.
6. Жмуров Д. В. Даркнет как ускользающая сфера правового регулирования // Сибирские уголовно-процессуальные и криминалистические чтения. — 2020. — № 1 (27). — С. 89–98.
7. Каримов В. Х. Актуальные вопросы выявления и расследования преступлений, совершаемых с использованием средств шифрования данных в сети Интернет // Уголовно-процессуальные и криминалистические чтения на Алтае : сборник науч. статей. Вып. 14 «Проблемы противодействия киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами». — Барнаул : Изд-во АлтГУ, 2017. — С. 40–48.
8. Лазаренко А. В. Технологии деанонимизации пользователей TOR // Новые информационные технологии в автоматизированных системах. — 2016. — № 19. — С. 257–262.
9. Сетько А. А., Швец Ю. Н. Darknet — одна из сторон интернета // Наука — образованию, производству, экономике : материалы XXII (69) Региональной научно-практической конференции преподавателей, научных сотрудников и аспирантов : в 2 т. — Витебск : Изд-во Витебского государственного университета имени П. М. Машерова, 2017. — С. 78–80.
10. Тадтаев Г., Костина Е. В деле математика Богатова сменился обвиняемый // Сайт RBC. URL: https://rbc-ru.turbopages.org/turbo/rbc.ru/s/society/21/05/2018/5b029a299a79470316d5afba?utm_source=turbo_turbo (дата обращения: 25.04.2021).
11. Узденов Р. М. Новые границы киберпреступности // Всероссийский криминологический журнал. — 2016. — Т. 10. — № 4. — С. 649–655.
12. Что такое глубокий и теневой интернет? // URL: <https://kaspersky-ru.turbopages.org/kaspersky.ru/s/resource-center/threats/deep-web> (дата обращения: 22.04.2021).

²⁷ Brauer J. LKA-RP: Großer Ermittlungserfolg von Generalstaatsanwaltschaft Koblenz und Zentraler Kriminalinspektion Oldenburg // URL: <https://www.presseportal.de/blaulicht/pm/29763/4809619> (дата обращения: 25.04.2021).

13. Brauer J. LKA-RP: Großer Ermittlungserfolg von Generalstaatsanwaltschaft Koblenz und Zentraler Kriminalinspektion Oldenburg // Presseportal. — URL: <https://www.presseportal.de/blaulicht/pm/29763/4809619> (дата обращения: 25.04.2021).
14. Taking Stock of the Online Drugs Trade / S. Hoorens, K. Kruithof [et al.] // URL: <https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html> (дата обращения: 23.04.2021).
15. Techniques and Applications for Crawling, Ingesting and Analyzing Blockchain Data / E. Brinckman, A. Kuehlkamp [et al.] // Сайт ResearchGate. — URL: https://www.researchgate.net/publication/335989766_Techniques_and_Applications_for_Crawling_Ingesting_and_Analyzing_Blockchain_Data (дата обращения 03.05.2021).

Материал поступил в редакцию 5 мая 2021 г.

REFERENCES (TRANSLITERATION)

1. Boj s ten'yu // Sajt kompanii «Oksidzen Softver». — URL: <https://www.oxygensoftware.ru/ru/news/articles/341-darknet> (data obrashcheniya: 24.04.2021).
2. Bondarenko Yu. A., Kizilov G. M. Problemy vyavleniya i ispol'zovaniya sledov prestuplenij, ostavlyаемых v seti Darknet // Gumanitarnye, social'no-ekonomicheskie i obshchestvennye nauki. — 2019. — № 5. — S. 97–101.
3. Vasil'ev A., Ibragimov Zh., Vasil'eva O. Darknet kak uskol'zayushchaya sfera pravovogo regulirovaniya // Yurisl'ingvistika. — 2019. — № 12. — S. 11–13.
4. Voksanaev V. P. Razvedka po otkryтым istochnikam: uroki proshlogo. — Ryazan': Poverennyj, 2007. — 174 s.
5. Konkurentnaya razvedka v komp'yuternyh setyah / A. G. Dodonov, D. V. Lande [i dr.]. — Kiev: IPRI NAN Ukrainy, 2013. — 250 s.
6. Zhmurov D. V. Darknet kak uskol'zayushchaya sfera pravovogo regulirovaniya // Sibirskie ugovolno-processual'nye i kriminalisticheskie chteniya. — 2020. — № 1 (27). — S. 89–98.
7. Karimov V. H. Aktual'nye voprosy vyavleniya i rassledovaniya prestuplenij, sovershaemyh s ispol'zovaniem sredstv shifrovaniya dannyh v seti Internet // Ugovolno-processual'nye i kriminalisticheskie chteniya na Altae: sbornik nauch. statej. Vyp. 14 «Problemy protivodejstviya kiberprestupnosti ugovolno-processual'nymi, kriminalisticheskimi i operativno-rozysknymi sredstvami». — Barnaul: Izd-vo AltGU, 2017. — S. 40–48.
8. Lazarenko A. V. Tekhnologii deanonimizatsii pol'zovatelej TOR // Novye informacionnye tekhnologii v avtomatizirovannyh sistemah. — 2016. — № 19. — S. 257–262.
9. Set'ko A. A., Shvec Yu. N. Darknet — odna iz storon interneta // Nauka — obrazovaniyu, proizvodstvu, ekonomike: materialy XXII (69) Regional'noj nauchno-prakticheskoy konferencii prepodavatelej, nauchnyh sotrudnikov i aspirantov: v 2 t. — Vitebsk: Izd-vo Vitebskogo gosudarstvennogo universiteta imeni P. M. Masherova, 2017. — S. 78–80.
10. Tadaev G., Kostina E. V dele matematika Bogatova smenilsya obvinyаемым // Sajt RBC. URL: [https://rbc.ru.turbopages.org/turbo/rbc.ru/s/society/21/05/2018/5b029a299a79470316d5afba?utm_source=turbo_turbo](https://rbc.ru/turbopages.org/turbo/rbc.ru/s/society/21/05/2018/5b029a299a79470316d5afba?utm_source=turbo_turbo) (data obrashcheniya: 25.04.2021).
11. Uzdenov R. M. Novye granicy kiberprestupnosti // Vserossijskij kriminologicheskij zhurnal. — 2016. — T. 10. — № 4. — S. 649–655.
12. Chto takoe glubokij i tenevoj internet? // URL: <https://kaspersky-ru.turbopages.org/kaspersky.ru/s/resource-center/threats/deep-web> (data obrashcheniya: 22.04.2021).
13. Brauer J. LKA-RP: Großer Ermittlungserfolg von Generalstaatsanwaltschaft Koblenz und Zentraler Kriminalinspektion Oldenburg // Presseportal. — URL: <https://www.presseportal.de/blaulicht/pm/29763/4809619> (data obrashcheniya: 25.04.2021).
14. Taking Stock of the Online Drugs Trade / S. Hoorens, K. Kruithof [et al.] // URL: <https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html> (data obrashcheniya: 23.04.2021).
15. Techniques and Applications for Crawling, Ingesting and Analyzing Blockchain Data / E. Brinckman, A. Kuehlkamp [et al.] // Sajt ResearchGate. — URL: https://www.researchgate.net/publication/335989766_Techniques_and_Applications_for_Crawling_Ingesting_and_Analyzing_Blockchain_Data (data obrashcheniya 03.05.2021).